НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп'ютерного практикуму №4

ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ ЗАХИЩЕНИХ МЕСЕНЖЕРІВ

Виконали студенти
групи ФІ-32мн
Пелешенко Любов,
Панасюк Єгор,
Маринін Іван Павло

Перевірила:
Селюх П.В.

Київ — 2024

1

Тема роботи: Дослідження систем захисту захищених месенжерів типу Viber, WhatsApp, Skype, Telegram.

Мета роботи: Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP.

Хід роботи

Сучасні месенджери, такі як Viber, WhatsApp, Skype та Telegram, широко використовуються для обміну повідомленнями та здійснення дзвінків. Забезпечення конфіденційності та безпеки цих комунікацій є критично важливим, що досягається за допомогою різних криптографічних механізмів. Також важливим є розуміння їхніх протоколів, структури пакетів та характеристик систем є важливим для оцінки безпеки, ефективності та надійності цих платформ.

У цьому документі розглянуто та проаналізовано кожен з цих аспектів для зазначених додатків.

1.1 Viber

Viber впровадив наскрізне шифрування (E2EE) у 2016 році. Хоча точні деталі реалізації не були повністю розкриті, відомо, що Viber використовує концепції протоколу Double Ratchet, подібні до тих, що застосовуються в Signal. Це забезпечує динамічне оновлення ключів для кожного сеансу, підвищуючи безпеку комунікацій.

Протокол

Viber використовує власний протокол для обміну повідомленнями та дзвінками. У 2016 році Viber впровадив наскрізне шифрування (E2EE) для всіх повідомлень і дзвінків, базуючись на концепціях протоколу Signal, зокрема Double Ratchet алгоритму. Це забезпечує динамічне оновлення ключів для кожного сеансу, підвищуючи безпеку комунікацій.

Структура пакетів

Детальна інформація про структуру пакетів Viber не є публічно доступною через закритий характер протоколу. Відомо, що Viber використовує шифрування для всіх даних, що передаються, включаючи повідомлення, дзвінки та файли, що ускладнює аналіз структури пакетів без доступу до внутрішньої документації.

Характеристики системи

Viber підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами та стікерами. Додаток доступний на різних платформах, включаючи iOS, Android, Windows та macOS. Viber використовує серверну інфраструктуру для маршрутизації повідомлень та дзвінків, забезпечуючи високу якість зв'язку та швидку доставку повідомлень.

1.2 WhatsApp

WhatsApp інтегрував протокол Signal для забезпечення E2EE у 2016 році, що означає, що лише відправник і одержувач можуть читати повідомлення. Протокол Signal поєднує алгоритм Double Ratchet, попередні

ключі (prekeys) та потрійний обмін ключами на основі еліптичних кривих (3-DH), використовуючи Curve25519, AES-256 та HMAC-SHA256 як примітиви. Це забезпечує пряму та зворотну секретність, гарантуючи, що компрометація одного ключа не впливає на безпеку попередніх або наступних повідомлень.

Протокол

WhatsApp використовує протокол Signal для забезпечення E2EE у всіх комунікаціях. Протокол Signal поєднує алгоритм Double Ratchet, попередні ключі (prekeys) та потрійний обмін ключами на основі еліптичних кривих (3-DH), використовуючи Curve25519, AES-256 та HMAC-SHA256 як криптографічні примітиви. Це забезпечує пряму та зворотну секретність, гарантуючи, що компрометація одного ключа не впливає на безпеку попередніх або наступних повідомлень.

Структура пакетів

Структура пакетів у WhatsApp визначається протоколом Signal. Кожне повідомлення інкапсулюється в зашифрований пакет, який містить:

– Ідентифікатор відправника та одержувача.

– Зашифрований текст повідомлення.

– Криптографічні метадані, такі як ініціалізаційний вектор (IV) та цифровий підпис.

Ця структура забезпечує цілісність та конфіденційність повідомлень під час передачі.

Характеристики системи

WhatsApp підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами, стікерами та групові чати. Додаток доступний на платформах iOS, Android, Windows та macOS. WhatsApp використовує серверну інфраструктуру для маршрутизації повідомлень та дзвінків, а також для зберігання зашифрованих резервних копій повідомлень.

1.3 Skype

У 2018 році Skype додав функцію "приватних розмов яка використовує протокол Signal для E2EE. Однак ця функція не є стандартною для всіх розмов і повинна бути активована користувачами вручну. Це означає, що за замовчуванням комунікації в Skype не є наскрізно зашифрованими, і користувачі повинні свідомо обирати безпечніші опції для конфіденційних розмов.

Протокол

Skype використовує власний протокол для обміну повідомленнями та дзвінками. У 2018 році Skype додав функцію "приватних розмов яка використовує протокол Signal для E2EE. Однак ця функція не є стандартною для всіх розмов і повинна бути активована користувачами вручну.

Структура пакетів

Оригінальний протокол Skype використовував пропрієтарну структуру пакетів, яка включала:

– Заголовок з інформацією про тип пакета та його розмір.

– Поле даних, що містить зашифровану інформацію, таку як повідомлення або медіа-дані.

З впровадженням "приватних розмов"структура пакетів для цих розмов відповідає специфікаціям протоколу Signal, забезпечуючи E2EE для відповідних повідомлень.

Характеристики системи

Skype підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами та екранами, а також групові чати та конференції. Додаток доступний на різних платформах, включаючи iOS, Android, Windows, macOS та Linux. Skype використовує гібридну інфраструктуру, поєднуючи серверну та peer-to-peer архітектуру для забезпечення зв'язку між користувачами.

1.4 Telegram

Telegram пропонує два типи чатів: звичайні та "секретні чати". Секретні чати використовують власний протокол MTProto для E2EE, який забезпечує шифрування між відправником і одержувачем. Однак за замовчуванням звичайні чати не використовують E2EE, що означає, що повідомлення можуть бути доступні серверам Telegram. Це викликає занепокоєння щодо конфіденційності, оскільки користувачі повинні вручну обирати секретні чати для забезпечення повної безпеки.

Протокол

Telegram використовує власний протокол MTProto для обміну повідомленнями. Існують два типи чатів:

– **Звичайні чати**: Використовують клієнт-сервер-клієнт шифрування, де повідомлення зберігаються на серверах Telegram у зашифрованому вигляді.

– **Секретні чати**: Використовують E2EE, забезпечуючи шифрування повідомлень між відправником та одержувачем без зберігання на серверах.

MTProto використовує комбінацію симетричного та асиметричного шифрування, зокрема AES-256, RSA та алгоритм Диффі-Хеллмана для обміну ключами.

Структура пакетів

У Telegram структура пакетів залежить від типу чату:

– **Звичайні чати**: Повідомлення передаються через сервери Telegram у зашифрованому вигляді. Кожне повідомлення інкапсулюється в пакет, що містить:

– Ідентифікатор відправника та одержувача.

– Зашифрований текст повідомлення.

– Криптографічні метадані, такі як ініціалізаційний вектор (IV) та цифровий підпис.

– **Секретні чати**: Повідомлення передаються безпосередньо між клієнтами, минаючи сервери. Структура пакетів схожа на звичайні чати, але з додатковими механізмами для забезпечення E2EE, такими як використання одноразових ключів (one-time keys) та підтвердження автентичності за допомогою QR-кодів.

Характеристики системи

Telegram підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами, стікерами та групові чати. Додаток доступний на різних платформах, включаючи iOS, Android, Windows, macOS та Linux. Telegram

використовує серверну інфраструктуру для маршрутизації повідомлень та дзвінків, а також для зберігання зашифрованих резервних копій повідомлень у хмарі. Важливо зазначити, що секретні чати не підтримують резервне копіювання, що підвищує рівень безпеки.

1.5 Порівняльний аналіз

Можливості систем

– **Viber**: Підтримує текстові повідомлення, голосові та відеодзвінки, обмін файлами, стікерами та групові чати.

– **WhatsApp**: Забезпечує текстові повідомлення, голосові та відеодзвінки, обмін файлами, стікерами, статуси та групові чати.

– **Skype**: Пропонує текстові повідомлення, голосові та відеодзвінки, обмін файлами, емоції, екраноспільний доступ та групові чати.

– **Telegram**: Надає текстові повідомлення, голосові та відеодзвінки, обмін файлами, стікерами, канали, боти, секретні чати та групові чати.

Криптографічні механізми

– **Viber**: Viber використовує наскрізне шифрування (E2EE) для всіх повідомлень і дзвінків, впроваджене у 2016 році. Однак, деталі реалізації залишаються закритими, що ускладнює незалежний аудит безпеки.

– **WhatsApp**: WhatsApp впровадив E2EE у 2016 році, використовуючи протокол Signal, який базується на алгоритмі Double Ratchet для керування ключами шифрування. Це забезпечує високий рівень безпеки та конфіденційності.

– **Skype**: Skype використовує власний протокол для обміну повідомленнями та дзвінками. У 2018 році було додано функцію "приватних розмов яка використовує протокол Signal для E2EE. Однак, ця функція не є

стандартною для всіх розмов і повинна бути активована користувачами вручну, що може призвести до ненавмисного використання менш безпечних комунікацій.

– **Telegram**: Telegram використовує власний протокол MTProto для обміну повідомленнями. Секретні чати забезпечують E2EE, але за замовчуванням звичайні чати не шифруються наскрізно. Це означає, що сервери Telegram мають доступ до змісту звичайних чатів, що може становити ризик для конфіденційності, якщо користувачі не обирають секретні чати.

Рівень захищеності

– **Viber**: Використовує E2EE, але відсутність відкритої інформації про реалізацію ускладнює оцінку рівня безпеки.

– **WhatsApp**: Високий рівень безпеки завдяки використанню протоколу Signal. Однак, збір метаданих може становити загрозу конфіденційності.

– **Skype**: Приватні розмови забезпечують E2EE, але стандартні чати не мають такого захисту.

– **Telegram**: Секретні чати забезпечують E2EE, але звичайні чати не шифруються наскрізно, що може бути вразливістю.

Додаткові функції безпеки

– **Viber**: Блокування екрану.

– **WhatsApp**: Двофакторна аутентифікація.

– **Skype**: Блокування небажаних контактів.

– **Telegram**: Самознищування повідомлення.

Розуміння протоколів, структури пакетів та характеристик систем Viber, WhatsApp, Skype та Telegram є важливим для оцінки їх безпеки та

ефективності. Хоча всі розглянуті месенджери впровадили певні форми шифрування для захисту комунікацій, існують значні відмінності в їх підходах та рівнях безпеки. WhatsApp забезпечує E2EE за замовчуванням для всіх повідомлень, використовуючи перевірений протокол Signal, що надає високий рівень безпеки. Viber та Skype також використовують протокол Signal або його елементи, але в Skype ця функція не є стандартною, а в Viber деталі реалізації не повністю відомі. Telegram, з іншого боку, використовує власний протокол для E2EE, але лише в секретних чатах, що вимагає від користувачів свідомого вибору для забезпечення повної конфіденційності.

WhatsApp та секретні чати Telegram забезпечують високий рівень безпеки завдяки використанню сучасних криптографічних протоколів. Однак, збір метаданих та відсутність наскрізного шифрування за замовчуванням у деяких випадках можуть становити загрозу конфіденційності. Вибір месенджера повинен базуватися на балансі між зручністю використання та вимогами до безпеки.

1.6 Рекомендації щодо безпечного використання месенджерів

Забезпечення безпеки під час використання месенджерів є критично важливим для захисту особистих даних та конфіденційності спілкування. Нижче наведено детальні рекомендації, які допоможуть користувачам підвищити рівень безпеки під час використання популярних месенджерів.

1) **Вибір безпечного месенджера**: Обирайте месенджери, які підтримують наскрізне шифрування (E2EE) за замовчуванням. Такі додатки, як Signal та WhatsApp, забезпечують високий рівень захисту повідомлень.

2) **Налаштування конфіденційності**: Перевірте та налаштуйте параметри конфіденційності у вашому месенджері:

а) Приховайте номер телефону: У деяких месенджерах можна налаштувати, хто може бачити ваш номер телефону. Рекомендується

обмежити цей доступ лише для контактів.

б) Обмежте видимість особистої інформації: Налаштуйте, хто може бачити вашу фотографію профілю, статус та інші особисті дані. Рекомендується встановити ці параметри на "Мої контакти"або "Ніхто".

3) **Використання двофакторної аутентифікації**: Увімкніть двофакторну аутентифікацію (2FA) у месенджері. Це додатковий рівень захисту, який вимагає введення додаткового коду під час входу, що ускладнює несанкціонований доступ до вашого облікового запису.

4) **Обережність з посиланнями та файлами**: Не відкривайте посилання чи файли, отримані від невідомих або неперевірених контактів. Це може запобігти встановленню шкідливого програмного забезпечення на ваш пристрій.

5) **Оновлення програмного забезпечення**: Регулярно оновлюйте месенджери та операційну систему вашого пристрою. Оновлення часто містять виправлення вразливостей, що підвищує загальний рівень безпеки.

6) **Використання окремого номера телефону**: Розгляньте можливість використання окремого номера телефону для реєстрації в месенджерах, особливо якщо ви використовуєте їх для професійних або чутливих комунікацій. Це допоможе зменшити ризик компрометації особистих даних.

7) **Захист від фішингу**: Будьте обережні з повідомленнями, що містять запити на надання особистої інформації або перенаправляють на підозрілі вебсайти. Завжди перевіряйте достовірність таких запитів.

8) **Використання безпечних з'єднань**: Під час використання месенджерів уникайте підключення до публічних Wi-Fi мереж без використання віртуальної приватної мережі (VPN). Це допоможе запобігти перехопленню ваших даних.

9) **Обмеження доступу до месенджера**: Використовуйте функції блокування додатка паролем або біометричними даними, якщо такі доступні. Це забезпечить додатковий захист у разі фізичного доступу до вашого пристрою.

10) **Освіта та обізнаність**: Постійно підвищуйте свою обізнаність щодо нових загроз та методів захисту в цифровому середовищі. Регулярно ознайомлюйтесь з рекомендаціями фахівців з кібербезпеки та дотримуйтесь їхніх порад.

Дотримання цих рекомендацій допоможе забезпечити безпечне та конфіденційне спілкування через месенджери, захистивши ваші особисті дані від потенційних загроз.

ВИСНОВКИ

У ході проведеного дослідження було здійснено детальний аналіз популярних систем обміну повідомленнями, таких як Viber, WhatsApp, Skype та Telegram. Розглянуто їхні функціональні можливості, криптографічні механізми та рівень захищеності. Встановлено, що кожна з цих платформ має свої переваги та недоліки в аспекті безпеки та конфіденційності користувачів. Зокрема, WhatsApp та Signal забезпечують наскрізне шифрування за замовчуванням, що гарантує високий рівень захисту повідомлень. Telegram пропонує опцію секретних чатів з наскрізним шифруванням, однак за замовчуванням повідомлення зберігаються на серверах у незашифрованому вигляді. Viber також використовує наскрізне шифрування, але існують питання щодо його реалізації та прозорості. Skype не надає наскрізного шифрування для всіх видів комунікації, що може бути вразливим місцем у забезпеченні конфіденційності. На основі отриманих даних розроблено рекомендації для користувачів щодо безпечного використання цих платформ, зокрема вибір месенджерів з надійними криптографічними механізмами, налаштування параметрів конфіденційності, увімкнення двофакторної аутентифікації та обережність при взаємодії з невідомими контактами. Дотримання цих порад сприятиме підвищенню рівня безпеки та захисту особистих даних під час використання месенджерів.